AMENDMENTS TO THE CLAIMS

Claims 1-40 were pending at the time of the Final Office Action.

Claims 1-8, 10-18, 20-36, and 38-39 are amended.

Claim 9 is canceled.

Claims 1-8 and 10-40 are now pending.

1. (Currently Amended) A method, comprising:

   analyzing a transport stream that includes one or more header portions and one or more corresponding payload portions, each of the header portions includes at least one of a packtetized elementary stream (PES) header and a frame header, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and

   preparing the transport stream for a data extraction~~ processing that bypasses encrypted portions of the transport stream~~ by encrypting at least some of the payload portions, while leaving the one or more corresponding header portions unencrypted at all times.

2. (Currently Amended) A method according to Claim 1, wherein analyzing the transport stream includes determining which of the one or more payload portions of the transport stream are to pass unencrypted.

3. (Currently Amended) A method according to Claim 2, wherein determining which of the one or more payload portions of the transport stream are to pass unencrypted is executed based on a statistical analysis.

4. (Currently Amended) A method according to Claim 2, wherein determining which of the one or more payload portions of the transport stream are to pass unencrypted is executed dynamically.

5. (Currently Amended) A method according to Claim 2, wherein determining which of the one or more payload portions of the transport stream are to pass unencrypted includes determining a permissible incursion beyond a~~ packet~~

header portion into a corresponding payload portion to gather data for the data extraction ~~processing~~.

6. (Currently Amended) A method according to Claim 2, wherein determining which of the one or more payload portions of the transport stream are to pass unencrypted includes detecting a data packet containing at least a portion of a PES ~~packetized elementary stream (PES)~~ header.

7. (Currently Amended) A method according to Claim 2, wherein determining which of the one or more payload portions of the transport stream are to pass unencrypted includes detecting whether each of the payload portions is in the same data packet as one of the one or more header portions ~~bytes of data that are required for processing the transport stream~~.

8. (Currently Amended) A method according to Claim 1, wherein preparing the transport stream for ~~processing~~ the data extraction further includes encrypting at least some of the payload portions that comprise payload data packets ~~of the transport stream that are not to pass unencrypted~~.

9. (Canceled).

10. (Currently Amended) A method according to Claim 1, wherein the one or more header portions and the one or more payload portions include data packets, and wherein preparing the transport stream for the data extraction ~~processing~~ further includes leaving a data packet containing at least a portion of a frame header unencrypted.

11. (Currently Amended) A method according to Claim 1, wherein ~~preparing the transport stream for processing includes leaving bytes of data unencrypted that are required for processing the transport stream~~ the data extraction includes bypasses encrypted portions of the transport stream to implement one of demultiplexing and indexing the transport stream for at least one of trick modes and thumbnail extraction.

12. (Currently Amended) A method according to Claim 1, wherein the payload portions include packets of PES payload data, and wherein preparing the transport stream for the data extraction ~~processing~~ includes common scrambling at least some of the packets ~~composed~~ of PES payload data.

13. (Currently Amended) A method according to Claim 1, wherein preparing the transport stream for the data extraction~~processing~~ includes:

generating a multiplex-compliant encryption method packet; and

inserting the multiplex-compliant encryption method packet into the transport stream.

14. (Currently Amended) A method according to Claim 13, wherein the encryption method packet identifies an encryption algorithm used in preparing the transport stream for the data extraction, the encryption method packet~~processing,~~ identifies encrypted portions of the transport stream, and provides data for deriving a decryption key.

15. (Currently Amended) A method according to Claim 13, wherein the encryption method packet identifies an unencrypted portion of the transport stream, a location of the encrypted portion~~of the unencrypted portion~~ of the transport stream, and a process corresponding to the unencrypted portion of the transport stream.

16. (Currently Amended) A method according to Claim 1~~Claim 13~~, wherein preparing the transport stream for the data extraction includes:

generating a multiplex-compliant encryption method packet; and

delivering the multiplex-compliant encryption method packet~~the encryption method packet is delivered~~ via a private table.

17. (Currently Amended) A method, comprising:

receiving a partially encrypted transport stream that includes one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more encrypted payload portions, wherein each of the unencrypted header portions enables the processing of the one or more corresponding encrypted payload portions based on at least one of the PES header and the frame header; and

extracting data from~~processing~~ the transport stream in a manner that bypasses the one or more encrypted payload portions of the transport stream.

18. (Currently Amended) A method according to Claim 17, further comprising:

receiving a multiplex-compliant encryption method packet corresponding to the transport stream; and

decrypting encrypted payload portions of the transport stream using a decryption key.

19. (Original) A method according to Claim 18, wherein the decryption key is included in the encryption method packet or is received in an out-of-band message.

20. (Currently Amended) A method according to Claim 17, wherein extracting data from ~~processing~~ the transport stream includes demultiplexing the transport stream based on unencrypted header portions of the transport stream.

21. (Currently Amended) A method according to Claim 17, wherein extracting data from ~~processing~~ the transport stream includes indexing payload data contained in the transport stream based on unencrypted header portions of the transport stream.

22. (Currently Amended) A computer-readable storage medium having one or more instructions that are executable by one or more processors, the one or more instructions causing the one or more processors to:

analyzing a transport stream that includes one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header ~~determine which portions of a transport stream are to pass unencrypted for processing that disregards encrypted portions of the transport stream~~; and

prepare the transport stream for ~~the processing~~ a data extraction by encrypting at least some of the payload portions while leaving the one or more corresponding header portions unencrypted.

23. (Currently Amended) A computer-readable storage medium according to Claim 22, wherein the one or more instructions to analyze the ~~determine which portions of the~~ transport stream ~~are to pass unencrypted~~ cause the one or more processors to leave unencrypted data packets having at least a portion of ~~a~~ the PES header.

24. (Currently Amended) A computer-readable storage medium according to Claim 22, wherein the one or more instructions to analyze the ~~determine which portion of the~~ transport stream ~~are to pass unencrypted~~ cause the one or more processors to leave unencrypted bytes of data required for processing the transport stream.

25. (Currently Amended) A computer-readable storage medium according to Claim 22, wherein the one or more instructions to analyze the ~~determine which portions of the~~ transport stream ~~are to pass unencrypted~~ cause the one or more processors to leave unencrypted a threshold amount of data beyond packet header data that is relevant for the processing.

26. (Currently Amended) A computer-readable storage medium according to Claim 22, wherein the one or more instructions to prepare the transport stream for the processing cause the one or more processors to encrypt at least some of the payload portions that comprise payload data packets ~~of the transport stream that are not to pass unencrypted~~.

27. (Currently Amended) A computer-readable storage medium according to Claim 26, wherein the one or more instructions causing the one or more processors to encrypt portions of the transport stream applies an advanced encryption standard (AES)-counter (CTR) mode cipher.

28. (Currently Amended) A computer-readable storage medium according to Claim 26, comprising one or more further instructions causing the one or more processors to:

generate a multiplex-compliant encryption method packet; and

insert the multiplex-compliant encryption method packet into the transport stream.

29. (Currently Amended) A computer-readable storage medium according to Claim 22, wherein the encryption method packet identifies an encryption algorithm used to prepare the transport stream for processing, identifies encrypted portions of the transport stream, and provides at least a basis for key to decrypt the encrypted portions of the transport stream.

30. (Currently Amended) A computer-readable storage medium according to Claim 22, wherein the encryption method packet identifies an unencrypted portion of the transport stream, a location of the unencrypted portion of the transport stream, and a process associated with the unencrypted portion of the transport stream.

31. (Currently Amended) A computer-readable storage medium having one or more instructions that are executable by one or more processors, the one or more instructions causing the one or more processors to:

receive a partially encrypted transport stream that includes one or more unencrypted header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions, and one or more encrypted payload portions, wherein each of the unencrypted header portions enables the processing of the one or more corresponding encrypted payload portions based on at least one of the PES header and the frame header; and

extract data from ~~process~~ the transport stream based on the one or more unencrypted header portions of the transport stream.

32. (Currently Amended) A computer-readable storage medium according to Claim 31, comprising one or more further instructions causing the one or more processors to:

receive a multiplex-compliant encryption method packet corresponding to the transport stream; and

decrypt encrypted payload portions of the transport stream using an encryption key based in the encryption method packet.

33. (Currently Amended) A computer-readable storage medium according to Claim 31, wherein the one or more instructions to process the transport stream cause the one or more processors to demultiplex the transport stream based on unencrypted header portions of the transport stream.

34. (Currently Amended) A computer-readable storage medium according to Claim 31, wherein the one or more instructions to process the transport stream cause the one or more processors to index payload data contained in the transport stream based on unencrypted header portions of the transport stream.

35. (Currently Amended) An apparatus, comprising:

an analyzer to determine which portions of a transport stream are to pass unencrypted ~~for processing that does not incorporate encrypted portions of the transport stream~~, wherein the analyzer identifies one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions in the transport stream, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and

a scrambler to encrypt at least some of the payload portions while leaving the one or more corresponding header portions unencrypted ~~other portions of the transport stream~~ based on the determination.

36. (Currently Amended) An apparatus according to Claim 35, wherein the analyzer is to dynamically determine that a threshold incursion into one payload portion~~data~~ is to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream.

37. (Original) An apparatus according to Claim 35, wherein the analyzer is to determine that a packet containing at least a portion of a PES header is to pass unencrypted.

38. (Currently Amended) An apparatus according to Claim 35, wherein the one or more payload portions include PES payload data, and wherein the analyzer is to determine that data arbitrarily disposed throughout PES payload data are to pass unencrypted.

39. (Currently Amended) An apparatus, comprising:

means for determining which portions of a transport stream are to pass unencrypted ~~for processing that does not incorporate encrypted portions of the transport stream~~, wherein the analyzer identifies one or more header portions, each of the one or more header portions being unencrypted at all times and including at least one of a packtetized elementary stream (PES) header and a frame header, and one or more payload portions in the transport stream, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on at least one of the PES header and the frame header; and

means for encrypting at least some of the payload portions while leaving the one or more corresponding header portions unencrypted ~~other portions of the transport stream~~ in accordance with the determination ~~analysis~~.

40. (Original) An apparatus according to Claim 39, wherein the means for determining designates a dynamically determined amount of payload data to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream.